NOUVELLES ANNALES DE MATHÉMATIQUES

A. LAISANT
ÉTIENNE BEAUJEUX

Mémoire sur certaines propriétés des résidus numériques

Nouvelles annales de mathématiques 2^e série, tome 9 (1870), p. 354-360

<http://www.numdam.org/item?id=NAM_1870_2_9__354_0>

MÉMOIRE SUR CERTAINES PROPRIÉTÉS DES RÉSIDUS NUMÉRIQUES

(suite et fin, voir 2e série, t. IX, p. 221, 271 et 302);

PAR MM. A. LAISANT ET ÉTIENNE BEAUJEUX.

21. Si l'on suppose que le nombre des restes composant la période soit *pair* et égal à $2n$, on voit qu'en conservant les notations employées précédemment on aura

$$A q^{2n} = m.D + A,$$

d'où

$$q^{2n} - 1 = m.D.$$

Par conséquent, si D est premier, $q^n - 1 = m.D$, ou $q^n + 1 = m.D$. Mais cette dernière égalité peut seule exister, car de la première résulterait que la période ne serait que de n termes. Donc aussi

$$q^{n+p} + q^p = m.D,$$
$$A q^{n+p} + A q^p = m.D,$$

et

$$r_{n+p} + r_p = m.D.$$

Or r_{n+p} et r_p étant plus petits que D, on ne peut avoir que

$$r_{n+p} + r_p = D.$$

Ainsi, *la somme des restes de même rang dans chaque demi-période est égale au diviseur, lorsque ce diviseur est un nombre premier.*

22. Dans cette même hypothèse d'un nombre pair $2n$ de termes à la période, on aura encore les propriétés suivantes :

1° *La somme des restes affectés d'indices impairs est un multiple du diviseur, et, par suite, il en est de même de la somme des restes d'indices pairs.*

En effet, $r_1 + r_3 + \ldots + r_{2n-1}$ peut être remplacé, à un multiple près de D, par

$$Aq + Aq^3 + \ldots + Aq^{2n-1} = Aq\left(\frac{q^{2n}-1}{q^2-1}\right);$$

donc, etc.

2° *Les termes de la suite $q, q^2, \ldots$, divisés par* D, *nombre premier, donnant lieu aux restes $r_1, r_2, r_3, \ldots$, et $2n$ étant le nombre des termes de la période, on aura $r_k^n = m.D \pm 1$, suivant que k est pair ou impair.*

Car (12) $r_k^n = r_n^k$, à un multiple près de D, et $r_n = D - 1$; donc, etc.

3° *n étant impair, on aura $r_p^k \pm r_{n+k}^{n+p} = m.D$, suivant que k et p sont de même parité ou de parités contraires.*

En effet (12), on a, à des multiples de D près,

$$r_{n+k} = r_n \times r_k,$$

d'où

$$\begin{aligned} r_{n+k}^{n+p} &= r_n^{n+p} \times r_k^{n+p} \\ &= r_n^n \times r_n^p \times r_k^n \times r_k^p \\ &= r_n^n \times r_n^p \times r_n^k \times r_k^p \\ &= r_n^{n+p+k} \times r_k^p; \end{aligned}$$

de là

$$\begin{aligned} r_k^p + r_{k+n}^{p+n} &= r_k^p\left(1 + r_n^{n+p+k}\right), \\ r_k^p - r_{k+n}^{p+n} &= r_k^p\left(1 - r_n^{n+p+k}\right); \end{aligned}$$

donc, etc.

4° *n étant pair, on aura $r_k^p \pm r_{n+k}^{n+p} = m.D$, suivant que k et p sont de parités contraires ou de même parité.*

On le verrait d'une façon analogue.

5° *n étant impair, si l'on écrit* $2n$ *restes consécutifs quelconques, le premier étant d'indice impair, qu'on élève celui-ci à la puissance* 1, *le second à la puissance* 2, *et ainsi de suite, la somme sera un multiple du diviseur.*

6° *Si n est pair, la même propriété aura lieu, mais en commençant par un reste d'indice pair.*

Ces deux dernières remarques sont des corollaires immédiats des deux précédents.

7° *La somme ou la différence des puissances pareilles de deux restes distants de n rang est un multiple du diviseur, selon que l'exposant de la puissance est impair ou pair.*

Cela résulte immédiatement de ce que $r_{n+k} = \mathrm{D} - r_k$.

8° *Soit n pair et égal à* $2n'$; *si l'on fait les deux produits* $r_k \times r_{k+1}$ *et* $r_{k+n'} \times r_{k+n'+1}$, *leur somme sera un multiple du diviseur.*

Car ces deux produits peuvent être remplacés par q^{2k+1} et $q^{2k+2n'+1}$, dont la somme est

$$q^{2k+1}(q^n + 1) = m.\mathrm{D}.$$

9° *Si l'on écrit les* $2n$ *restes sur deux lignes horizontales*

$$r_1, \quad r_2, \ldots, \quad r_n,$$
$$r_{n+1}, \quad r_{n+2}, \ldots, \quad r_{2n},$$

la somme des produits indiqués est un multiple du diviseur.

En effet,

$$r_{n+k} = \mathrm{D} - r_k;$$

donc

$$r_{n+k} \times r_k = m.\mathrm{D} - r_k^2;$$

d'où résulte que, pour la somme, on aura

$$m.\mathrm{D} - (r_1^2 + r_2^2 + r_3^2 + \ldots + r_n^2).$$

En remplaçant r_1 par q, r_2 par q^2, ..., tout se réduit à examiner l'expression

$$q^2 + q^4 + \ldots + q^{2n},$$

ou la suivante

$$1 + q^2 + \ldots + q^{2n-2} = \frac{q^{2n} - 1}{q^2 - 1} = m.\mathrm{D}.$$

Donc, etc.

10° *n étant pair et égal à* $2n'$, *écrivons comme ci-dessous les* $4n$ *restes :*

$$\text{(A)} \quad \begin{cases} r_1 & r_2, \ldots, & r_{n'}, \\ r_{n'+1}, & r_{n'+2}, \ldots, & r_{2n'}, \end{cases}$$

$$\text{(B)} \quad \begin{cases} r_{2n'+1}, & r_{2n'+2}, \ldots, & r_{3n'}, \\ r_{3n'+1}, & r_{3n'+2}, \ldots, & r_{4n'}. \end{cases}$$

Si l'on fait les produits indiqués en (A) *et* (B) *et leurs sommes respectives* P *et* L, *on aura*

$$\mathrm{P} - \mathrm{L} = m.\mathrm{D};$$

car $r_k \times r_{n'+k}$ et $r_{2n'+k} \times r_{3n'+k}$ peuvent être remplacés respectivement par $q^{2k+n'}$ et par $q^{2k+3n'}$ ou par $r_{2k+n'}$ et $r_{2k+3n'}$, et, de plus, $r_{2k+n'} = r_{2k+3n'}$; donc, etc.

11° *Soit toujours* $n = 4n'$, *et posons*

$$\begin{aligned} r_1 + \ldots + r_{n'} &= \mathrm{S}_1, \\ r_{n'+1} + \ldots + r_{2n'} &= \mathrm{S}_2, \\ r_{2n'+1} + \ldots + r_{3n'} &= \mathrm{S}_3, \\ r_{3n'+1} + \ldots + r_{4n'} &= \mathrm{S}_4; \end{aligned}$$

on aura

$$\begin{aligned} \mathrm{S}_1\mathrm{S}_3 + \mathrm{S}_2\mathrm{S}_4 &= m.\mathrm{D}, \\ \mathrm{S}_1\mathrm{S}_4 - \mathrm{S}_2\mathrm{S}_3 &= m.\mathrm{D}, \\ \mathrm{S}_1\mathrm{S}_2 - \mathrm{S}_3\mathrm{S}_4 &= m.\mathrm{D}. \end{aligned}$$

On le voit sans peine en remplaçant S_1, S_2, S_3, S_4 par

$$q\left(\frac{q^{n'}-1}{q-1}\right),\ q^{n'+1}\left(\frac{q^{n'}-1}{q-1}\right),\ q^{2n'+1}\left(\frac{q^{n'}-1}{q-1}\right),\ q^{3n'+1}\left(\frac{q^{n'}-1}{q-1}\right)$$

respectivement.

12° *Supposons toujours* $n = 4n'$, *posons*

$$\begin{aligned} r_1 + r_3 + \ldots + r_{2n'-1} &= \Sigma_1, \\ r_2 + r_4 + \ldots + r_{2n'} &= \Sigma_2, \\ r_{2n'+1} + r_{2n'+3} + \ldots + r_{4n'-1} &= \Sigma_3, \\ r_{2n'+2} + r_{2n'+4} + \ldots + r_{4n'} &= \Sigma_4; \end{aligned}$$

on aura

$$\begin{aligned} \Sigma_1\Sigma_2 - \Sigma_3\Sigma_4 &= m.\mathrm{D}, \\ \Sigma_1\Sigma_4 - \Sigma_2\Sigma_3 &= m.\mathrm{D}. \end{aligned}$$

On s'en assurerait comme précédemment.

Nota. On verrait aisément que plusieurs des propriétés de ce numéro s'étendent aux restes dus à la progression géométrique Aq, $Aq^2, \ldots$, où A est différent de 1.

23. Pour terminer, nous proposerons au lecteur, à titre d'exercices, les questions suivantes :

1° En divisant les nombres q, $q^2, \ldots$ par un diviseur D qui s'écrive ab dans le système de numération de base q, démontrer que

$$\begin{aligned} a^2r_2 - b^2r_0 &= m.\mathrm{D}, \\ a^3r_3 - b^3r_0 &= m.\mathrm{D}, \\ a^4r_4 - b^4r_0 &= m.\mathrm{D}, \\ &\ldots\ldots\ldots\ldots, \end{aligned}$$

et ainsi de suite, r_0 étant un reste quelconque.

2° D, nombre premier, s'écrivant encore ab dans le système de base q, donne lieu, appliqué comme diviseur à la suite Aq, $Aq^2, \ldots$, à une période de $2n$ restes

$r_1, r_2, \ldots, r_{2n}$. Démontrer que

$$ar_k - br_{k+n-1} = m.\mathrm{D}$$

et

$$ar_{k+n+1} - br_k = m.\mathrm{D}.$$

3° En divisant q, $q^2, \ldots$ par le nombre premier, $\mathrm{D} = \frac{q + \mathrm{B}}{\mathrm{N}}$, qui s'écrit ab dans le système B, on trouve une période de $2n$ restes $r_1, \ldots, r_{2n}$. Démontrer que

$$ar_k + br_{k+n-1} = \mathrm{D}$$

et

$$ar_{k+n+1} + br_k = m.\mathrm{D}.$$

Si, au contraire, $\mathrm{D} = \frac{q - \mathrm{B}}{\mathrm{N}}$, on aura

$$ar_k - br_{k+n-1} = \mathrm{D}$$

et

$$ar_{k+n+1} - br_k = m.\mathrm{D}.$$

4° Soit $r_1, r_2, \ldots, r_{n-1}$ $(r_n = 1)$ la période obtenue en divisant q, $q^2, \ldots$ par D; faire voir que si l'on prend $\mathrm{Q} = m.\mathrm{D} + r_{n-1}$, on trouvera, en partant de Q, $\mathrm{Q}^2, \ldots$ la période précédente renversée, au dernier terme près qui reste le même $r_{n-1}, r_{n-2}, \ldots, r_1 (r_n = 1)$.

5° Soit $r_1, r_2, \ldots, r_n$ une suite quelconque de n restes consécutifs provenant de la division de q, q^2, $q^3, \ldots$ par un même diviseur, la période étant de n termes. Écrivons au-dessous une permutation circulaire quelconque de ces restes

$$r_1, \quad r_2, \ldots, \quad r_n,$$
$$r_p, \quad r_{p+1}, \ldots, \quad r_{p-1}.$$

Si l'on fait les produits indiqués, leur somme sera multiple de D, à la condition qu'on ait $n > 2$.

6° q, $q^2, \ldots$, divisés par D, donnant lieu à une période de n termes, formons un multiple de D qui ait

n chiffres dans le système de numération de base q. Soit $\alpha_n\ \alpha_{n-1}\ldots\ \alpha_1$ ce multiple. On sait qu'en écrivant $\alpha_1, \alpha_2, \ldots, \alpha_n$ sous n restes consécutifs quelconques, la somme des produits sera égale à un multiple du diviseur. Démontrer qu'il en est de même aussi en écrivant $\alpha_1 \pm r_1$, $\alpha_2 \pm r_2, \ldots, \alpha_n \pm r_n$, ou bien $\alpha_1 \pm k, \ldots, \alpha_n \pm k$, au lieu des chiffres $\alpha_1, \ldots, \alpha_n$ ($r_1, \ldots, r_n$ sont n restes consécutifs quelconques, k est un entier quelconque).